

REMARKS

By this amendment, Applicant adds new claims 16-20. Applicant submits that all new claims are fully supported in the originally filed specification and requests the entry and allowance of these claims. Therefore, claims 1-20 are all the claims pending in the application.

Rejection of claims 1-15 under § 103(a) over Van Buer in view of Takagi

Claims 1-15 are rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Van Buer (US Patent Publication No. 2003/0198345), hereafter “Van Buer”, in view of Takagi et al. (US Patent No. 6,259,790), hereafter “Takagi”. Applicant respectfully submits the following in traversal.

Claim 1

Applicant submits that claim 1 is patentable. The Examiner concedes that Van Buer does not explicitly disclose a coefficient table providing first to fourth coefficients in response to said row index. However, the Examiner cites Takagi to make up for the deficiency. Applicant disagrees with the Examiner for the following reasons.

Claim 1 recites an AES encryption processor comprising, *inter alia*, a coefficient table providing first to fourth coefficients in response to said row index. The Examiner cites col. 26, lines 54-67, col. 27, lines 1-5 and figure 13 of Takagi as allegedly disclosing the above claim feature. The Examiner alleges that the coefficient table memory unit 137c of figure 13 of Takagi corresponds to the claimed coefficient table. Applicant notes that Takagi discloses an upper digit encryption processing unit 137 using a RSA cryptosystem (col. 26, lines 9-12, this second embodiment is directed to an RSA type authentication system) and on the other hand, claim 1 recites an AES encryption processor. It is well known to one of ordinary skill in the art that a RSA is an asymmetric encryption algorithm and an AES is a symmetric encryption algorithm.

Since Takagi discloses an RSA upper digit encryption processor 137, Applicant respectfully submits that the upper digit encryption processing unit 137 comprising the coefficient table memory unit 137c does not correspond to the claimed AES processor comprising a coefficient table.

The Examiner concedes that Van Buer does not explicitly disclose a table providing first to fourth coefficients in response to said row index. However, the Examiner alleges that Van Buer discloses first to fourth multipliers respectively, computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients respectively. Applicant submits that the Examiner presents contradictory assertions. Applicant requests the Examiner clarify what the Examiner regards as corresponding to the claimed first to fourth multipliers respectively, computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients respectively.

In addition, claim 1 recites an AES encryption processor comprising, *inter alia*, an accumulator which accumulates the first to fourth products corresponding to all four columns of the state to develop first to fourth elements of a designed column of a resultant state. The Examiner cites paragraphs [0067] to [0070] of Van Buer as allegedly disclosing the above features of claim 1. Applicant respectfully disagrees for the following reasons.

The cited reference discloses a design for circuitry to perform substitution for both encryption and decryption in a single dual-mode pipeline 150 using a single octet table 152. It appears that the Examiner alleges that the MUX 158 of Fig. 4 of Van Buer corresponds to the claimed accumulator. However, Applicant notes that the MUX 158 merely adds the input octet (output from the S-box 152) to the affine transformation 160 (see Fig. 4 of Van Buer). As submitted in the response to the Office Action dated September 18, 2008, Applicant notes that

Figure 3 of Van Buer depicts one element (one octet) per one S-box. Therefore, the result of Fig. 4 is still one element (paragraph [0068] and Fig. 4 of Van Buer - “The second multiplexer 158 determines the proper output, the result of the S-box 152 for decryption or the output of the affine function performed in box 160 for encryption”). Since the MUX 158 merely outputs one element, Applicant respectfully submits that Van Buer fails to disclose or suggest “an accumulator which accumulates the first to fourth products corresponding to all four columns of the state to develop first to fourth elements of a designed column of a resultant state”.

Furthermore, Applicant reiterates the remarks made on January 16, 2009 in response to the Office Action dated September 18, 2008. Specifically, Applicant submits that Van Buer depicts a plurality of substitution boxes or S-boxes, S1 through S16, being used in parallel to process 16 octets of the input data (Fig. 3 of Van Buer). The parallel nature of processing in Van Buer is emphasized in paragraph 63: “processing the entire block 120 in parallel, as illustrated in Fig. 3”. Therefore, since Van Buer uses one S-box for every element, there is no need to use “an accumulator...to develop first to fourth elements of a designated column of a resultant state” as claimed in claim 1. (See also page 34, line 16 - page 35, line 13 of the originally filed specification discussing an exemplary embodiment of the present invention: “The architecture in this embodiment effectively reduces necessary hardware while achieving the parallel processing. The coefficient table 106, the multipliers 107₀ to 107₄, and the adder 109 eliminate the need for preparing a plurality of S-boxes (or expanded S-boxes) for implementing parallel processing in connection with a single column of the output state” and “the architecture in this architecture requires the single S-box 105 containing 256 8-bit words, that is, a 2 k-bit memory”).

For at least the reasons submitted above, Applicant respectfully submits that claim 1 is patentable.

For reasons similar to those submitted for claim 1, Applicant respectfully submits that claims 3, 6, 8, 15, 11, 12 and 14 are patentable.

Claims 2, 4, 5, 7, 9, 10, 13 and 15, which depend from claims 1, 3, 6, 8 or 12, are patentable at least by virtue of their dependencies.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

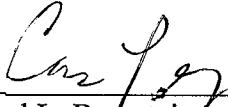
SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: July 27, 2009

 #46,766

Howard L. Bernstein
Registration No. 25,665